

[19]中华人民共和国专利局

[51]Int.Cl<sup>6</sup>

H04L 9/20



# [12] 发明专利申请公开说明书

[21] 申请号 97114947.X

[43]公开日 1998 年 1 月 21 日

[11] 公开号 CN 1170995A

[22]申请日 97.5.22

[30]优先权

[32]96.5.22 [33]JP[31]126751 / 96

[71]申请人 松下电器产业株式会社

地址 日本大阪府

[72]发明人 松崎夏生 原田俊治 馆林诚

[74]专利代理机构 中国专利代理(香港)有限公司

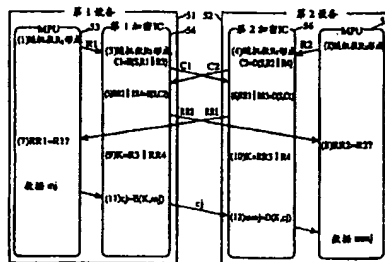
代理人 叶恺东 王忠忠

权利要求书 8 页 说明书 24 页 附图页数 11 页

[54]发明名称 保证设备之间通信安全的加密装置

[57]摘要

在第 1 设备 51 中, MPU53 形成作为询问数据的随机数 R1, 第 1 加密 IC54 将上述随机数 R1 和本身形成的数据传送键用的随机数 R3 结合并加密, 之后作为密码文字 C1 发送给第 2 设备 52。同样, 当接收第 2 设备 52 发送的密码文字 C2 时, 第 1 加密 IC54 对上述密码文字 C2 进行译码, 将其分成第 1 分离数据 RR2 和第 2 分离数据 RR4。第 1 加密 IC54 将第 1 分离数据 RR2 作为响应数据返回给第 2 设备 52。MPU53 对第 2 设备 52 返回的第 1 分离数据 RR1 和随机数 R1 进行比较, 在它们保持一致的场合, 认证第 2 设备 52 为正当的设备。



(BJ)第 1456 号

用在上述步骤(9)中所获得的数据传送键K对MPU73发出的分块数字作品mj(64位)进行加密,将所获得的密码文字Cj发送给第2设备72,直到可传送的全部数字作品的发送结束。

(12)与步骤(11)相对应,在第2设备72的第2加密IC76中,接收第1设备71发送的加密的上述数字作品Cj(64位),使用在步骤(10)所获得的数据传送键K进行译码,将所获得的数字作品mmj传送给MPU75。反复进行上述译码处理直至上述数字作品Cj全部从第1设备71发送过来。

按上述方式,通过第2实施例的加密装置,和第一实施例的场合同样,可在第1设备71和第2设备72之间进行相互认证、数据传送键K的共用、以及数据密码的通信。

另外,如上所述,对于本实施例与第1实施例的加密装置,它们的硬件结构相同,只是处理顺序,即每个硬件结构组成部分的连接和实现顺序不同。因此,可以说本实施例的加密装置的特征或其变换实例与第1实施例的场合相同。

### 15 (第3实施例)

上述的第1实施例和第2实施例中的加密装置具有下述的相同点。

(1)在双方的设备中,分别形成2个随机数,其中一个仅仅用于认证,而另一个仅仅用于形成数据传送键K。

(2)用于形成数据传送键K的随机数未按原样输出到加密IC的外部,而用于认证用的随机数则输出到加密IC的外部并公开。

与此相对,下面将要描述的第3实施例的加密装置仅仅形成一个随机数,该随机数同时用于认证和形成数据传送键。其原因是:与第1和第2实施例相比,可减轻加密IC内部随机数形成的负担。

另外,在加密IC的内部形成用于认证的随机数,并进行比较处理。即,与第1和第2实施例不同,通过加密IC内部电路,不仅形成数据传送键,而且还进行认证处理。其原因是:如上所述,要对付将加密IC用于密码译解的不正当使用,从而可提高密码通信的安全性。

图6为本发明第3实施例的加密装置的处理程序图,该实施例可在设置有本发明的加密装置的第1设备81和第2设备82之间进行相互认证、数据传送键的共用、以及数据的密码通信。

图 6 表示从第 1 设备 81 向第 2 设备 82 传送数字作品 mj 的场合。

另外, 在本实施例中, 与第 1 实施例和第 2 实施例相同, 设置于每个设备 81, 82 中的本发明加密装置从整体上看, 由 MPU83, 85, 以及加密 IC84, 86 构成。另外, 由于 MPU83, 85 具有仅仅把数字作品 mj 传送给加密 IC84, 86 的功能, 这样实质上本发明的加密装置仅仅由加密 IC84, 86 构成。

第 1 加密 IC84 和第 2 加密 IC86 与第 1 和第 2 实施例相同, 为单片的半导体 IC。

下面根据图 6 所示的步骤标号, 对第 3 实施例的加密装置的动作进行描述。

10 (1) 在第 1 加密 IC84 中, 产生随机数 R1, 将其存储起来, 通过 E 函数对其进行加密, 通过第 1 设备 81 中的发送部 (图中未示出) 将密码文字 C1 发送给第 2 设备 82。在加密过程中, 采用与第 2 加密 IC86 预先共同保持的秘密认证键 S。在第 2 设备 82 中, 将所接收的密码文字 C1 传送给第 2 加密 IC86。

15 (2) 在第 2 加密 IC86 中, 所接收的密码文字 C1 通过逆变换算法 D 译码, 获得译码文字 RR1。在第 1 加密 IC84 和第 2 加密 IC86 为正规部件的场合, 上述译码文字 RR1 与上述随机数 R1 保存一致。

(3) 在第 2 加密 IC86 中, 产生随机数 R2, 将其存储起来, 使其与上述译码文字 RR1 相结合, 并通过上述逆变换算法 D 译码。在译码过程中采用上述的认证键 S。第 2 加密 IC86 通过第 2 设备 82 中的发送部 (图中未示出) 将译码文字 C2 发送给第 1 设备 81。在第 1 设备 81 中, 将其传送给第 1 加密 IC84。

(4) 在第 1 加密 IC84 中, 通过 E 函数对上述译码文字 C2 进行加密, 将其分解为分离数据 RRR1 和分离数据 RR2。另外, 当分离数据 RRR1 通过正当的设备交换时, 上述译码文字 RR1 和随机数 R1 保持一致。另外, 分离数据 RR2 与上述随机数 R2 保持一致。

25 (5) 在第 1 加密 IC84 内部, 对通过上述步骤 (1) 存储的随机数 R1 和上述分离数据 RRR1 进行比较, 当它们保持一致时, 对第 2 加密 IC86 以及包括该第 2 加密 IC86 的第 2 设备 82 的正当性进行认证。

(6) 在第 1 加密 IC84 中, 通过上述 E 函数对上述分离数据 RR2 进行加密, 将其发送给第 2 设备 82。第 2 设备 82 将其密码文字 C3 传送给第 2 加密 IC86。

(7) 在第2加密 IC86 中, 通过上述逆变换算法 D 对上述密码文字 C3 进行译码, 从而获得译码文字 RRR2。

(8) 在第2加密 IC86 中, 对通过上述步骤(3)存储的随机数 R2 和上述译码文字 RRR2 进行比较, 当它们保持一致时, 对第1加密 IC84 以及包括该  
5 第1加密 IC84 的第1设备 81 的正当性进行认证。

(9) 在第1加密 IC84 中, 通过将上述随机数 R1 和上述分离数据 RR2 结合, 形成数据传送键 K。

(10) 在第2加密 IC86 中, 使用上述译码文字 RR1 和上述随机数 R2 形成数据传送键 K。

10 (11) 在第1设备 81 的第1加密 IC84 中, 反复进行下述的处理, 即使用在上述步骤(9)形成的数据传送键 K 对 MPU83 给出的分块数字作品 mj (64 位) 进行加密, 将所形成的密码文字 Cj 发送给第2设备 82, 直到可传送的全部数字作品的发送结束。

(12) 与步骤(11)相对应, 在第2设备的第2加密 IC86 中, 接收第1  
15 设备 81 所发送的加密的上述数字作品 Cj (64 位), 使用在上述步骤(10)形成的数据传送键 K 并进行译码处理, 将所形成的数据作品 mmj 传送给 MPU85。反复进行上述译码处理, 直至将上述数字作品 cj 从第1设备 81 全部发送过来。

按上述方式, 通过第3实施例的加密装置, 与第1和第2实施例相同, 可在第1设备 81 和第1设备 82 之间, 进行相互认证、数据传送键 K 的共用、以及  
20 数据密码的通信。

另外, 在上述步骤(1), (2), (6) 和(7)中进行一个随机数的加密, 在步骤(3), (4)中进行2个随机数的结合的加密。在采用64位宽度的 E 函数和逆变换算法 D 的场合, 也可使每个随机数为32位, 在前一情况中, 在输入剩余的32位时填充固定的32位值。比如, 将随机数定为下位32  
25 位, 使上位32位全部为固定值零等。另外, 对于后一情况, 也可将所结合的64位按照原样输入到每个函数中。

此外, 在每个随机数的位长度为64位的倍数时, 对于前者, 也可按照原样输入到函数中, 对于后者, 也可反复2次采用每个函数, 按照 CBC 的模式进行具有一定连锁性的加密。

30 在上述第3实施例中, 与第1和第2实施例不同, 其随机数同时用作认证

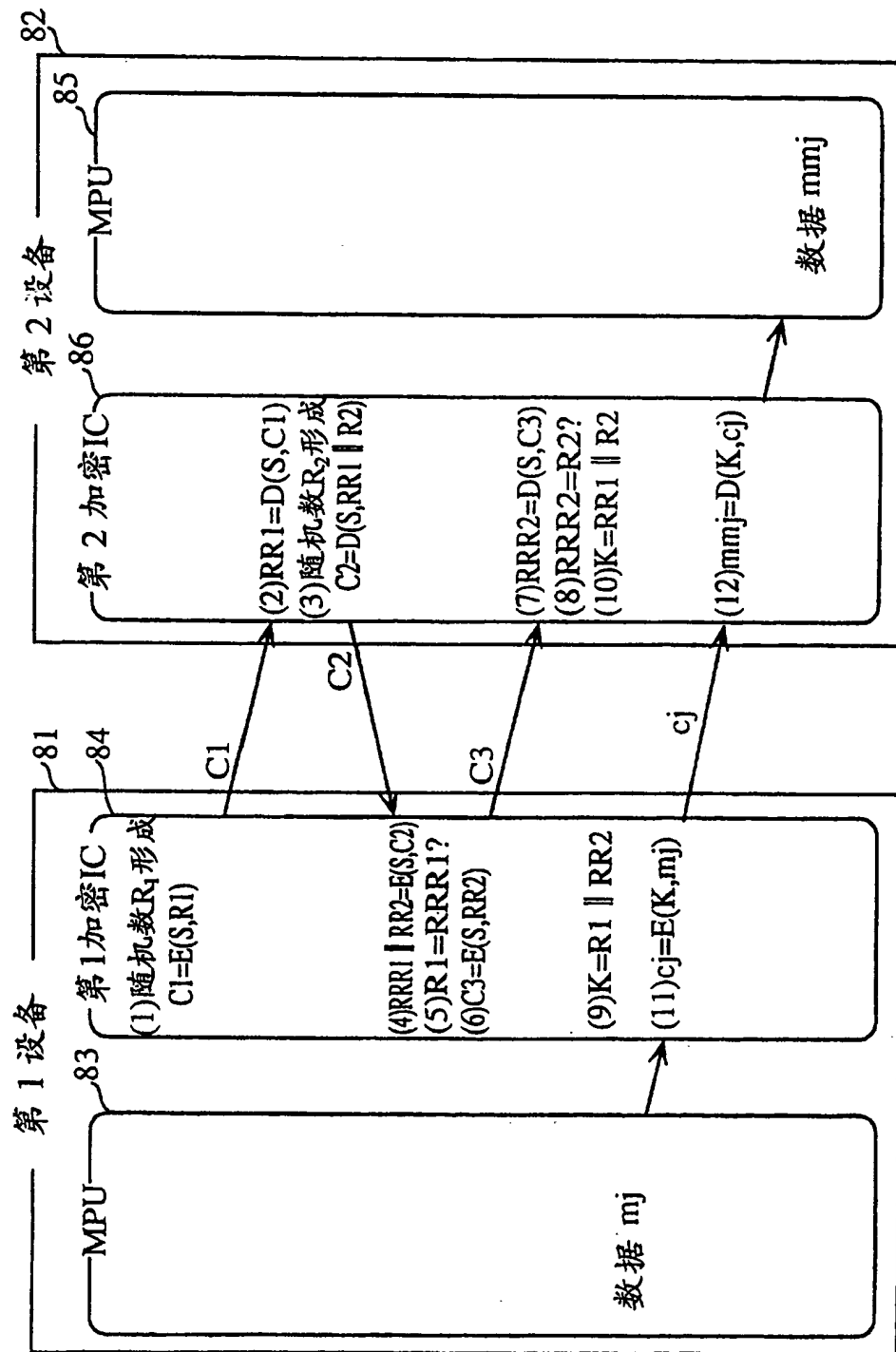


图 6